PATENT APPLICATION

#2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Masaki KYOJIMA and Kil-ho SHIN

Application No.: New U.S. Application

Filed: June 6, 2000 Docket No.: 106406

For: DATA GENERATING APPARATUS AND DATA VERIFYING APPARATUS

CLAIM FOR PRIORITY

Director of the U.S. Patent and Trademark Office
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

Japanese Patent Application No. 11-226380 filed August 10, 1999.

In support of this claim, a certified copy of said original foreign application:

__X__ is filed herewith.

_____ was filed on _____ in Parent Application No. _____ filed _____.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Thomas J. Pardini
Registration No. 30,411

JAO:TJP/emb

Date: June 6, 2000

DEPOSIT ACCOUNT USE AUTHORIZATION
Please grant any extension necessary for entry;
Charge any fee due to our Deposit Account No. 15-0461

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年　８月１０日

出 願 番 号
Application Number: 平成１１年特許願第２２６３８０号

出 願 人
Applicant (s): 富士ゼロックス株式会社

２０００年　４月２１日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号　出証特２０００－３０２８０１０

【書類名】　特許願

【整理番号】　FN99-00075

【提出日】　平成11年 8月10日

【あて先】　特許庁長官殿

【国際特許分類】　H04L　9/30

【発明の名称】　データ生成装置およびデータ検証装置ならびにその方法

【請求項の数】　32

【発明者】

【住所又は居所】　神奈川県足柄上郡中井町境４３０　グリーンテクなかい　富士ゼロックス株式会社内

【氏名】　京嶋　仁樹

【発明者】

【住所又は居所】　神奈川県足柄上郡中井町境４３０　グリーンテクなかい　富士ゼロックス株式会社内

【氏名】　申　吉浩

【特許出願人】

【識別番号】　000005496

【氏名又は名称】　富士ゼロックス株式会社

【電話番号】　0462-38-8516

【代理人】

【識別番号】　100086531

【弁理士】

【氏名又は名称】　澤田　俊夫

【電話番号】　03-5541-7577

【手数料の表示】

【予納台帳番号】　038818

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ生成装置およびデータ検証装置ならびにその方法

【特許請求の範囲】

【請求項１】　第１のデータを保持する主検査対象データ記憶部と、

第２のデータを保持する副検査対象データ記憶部と、

上記副検査対象データ記憶部に記憶されたデータから暗号鍵を作成する暗号鍵生成部と、

上記主検査対象データ記憶部に記憶されたデータを上記暗号鍵生成部が生成した暗号鍵で暗号化する暗号部とを備え、

上記暗号部で暗号化された結果および上記副検査対象データ記憶部に記憶されたデータの少なくとも一方を含むデータを作成することを特徴とするデータ生成装置。

【請求項２】　前鍵を保持する前鍵保持部を更に備え、上記暗号鍵生成部が暗号鍵を生成する際に、上記前鍵保持部に記憶された前鍵も使用することを特徴とする請求項１記載のデータ生成装置。

【請求項３】　上記主検査対象データ記憶部に記憶されるデータが、所定の暗号文を復号した結果であることを特徴とする請求項１記載のデータ生成装置。

【請求項４】　上記主検査対象データ記憶部に記憶されるデータが、所定のデータの署名値であることを特徴とする請求項１記載のデータ生成装置。

【請求項５】　上記暗号鍵生成部が一方向性関数で構成されており、該一方向性関数に上記副検査対象データ記憶部に記憶されたデータを入力して得られた結果が上記暗号鍵である請求項１記載のデータ生成装置。

【請求項６】　上記前鍵を暗号化するための前鍵暗号鍵を保持する前鍵暗号鍵記憶部と、前鍵暗号鍵記憶部に記憶された鍵で前鍵を暗号化する前鍵暗号部とを備えることを特徴とする請求項２記載のデータ生成装置。

【請求項７】　上記暗号部で行われる暗号化が、共通鍵暗号であることを特徴とする請求項１記載のデータ生成装置。

【請求項８】　上記暗号部で行われる暗号化が、所定の法数のもとでの上記主検査対象データ記憶部に記憶されているデータと、上記暗号鍵生成部で生成さ

れた暗号鍵の乗除演算であることを特徴とする請求項１記載のデータ生成装置。

【請求項９】　第１のデータから暗号鍵を作成するステップと、

所定の特徴を持つことが検査可能な第２のデータを該暗号鍵で暗号化するステップと、

第１のデータおよび暗号化された第２のデータの少なくとも一方を含むデータを作成するステップとからなるデータ生成方法。

【請求項１０】　第１のデータを保持する主検査対象データ記憶部と、

第２のデータを保持する副検査対象データ記憶部と、

上記副検査対象データ記憶部に記憶されたデータから復号鍵を作成する復号鍵生成部と、

上記主検査対象データ記憶部に記憶されたデータを上記復号鍵生成部が生成した復号鍵で復号する復号部と、

上記復号部で復号されたデータが所定の特徴を持つかどうかを検査する検査部とを備えることを特徴とするデータ検証装置。

【請求項１１】　前鍵を保持する前鍵保持部を更に備え、上記復号鍵生成部が復号鍵を生成する際に、上記前鍵保持部に記憶された前鍵も使用することを特徴とする請求項１０記載のデータ検証装置。

【請求項１２】　上記検査部が、上記復号部で復号されたデータが所定のデータを所定の復号鍵で復号した結果であることを検査することを特徴とする請求項第１０記載のデータ検証装置。

【請求項１３】　上記検査部が、上記復号部で復号されたデータが所定のデータを所定の署名鍵で署名した署名値であることを検査することを特徴とする請求項１０記載のデータ検証装置。

【請求項１４】　上記復号鍵生成部が一方向性関数で構成されており、該一方向性関数に上記副検査対象データ記憶部に記憶されたデータを入力して得られた結果が上記復号鍵である請求項１０記載のデータ検証装置。

【請求項１５】　暗号化された前鍵を記憶する前鍵記憶部と、

暗号化された上記前鍵を復号する復号鍵を記憶する前鍵復号鍵記憶部と、

上記前鍵復号鍵記憶部に記憶された上記復号鍵で上記前鍵記憶部に記憶された

暗号化された前鍵を復号する前鍵復号部とをさらに備えることを特徴とする請求項１０記載のデータ検証装置。

【請求項１６】　上記復号部で行われる復号が、共通鍵暗号の復号であることを特徴とする請求項１０記載のデータ検証装置。

【請求項１７】　上記復号部で行われる復号が、所定の法数のもとでの暗号化された被検査値と復号鍵の乗除算であることを特徴とする請求項１０記載のデータ検証装置。

【請求項１８】　第１のデータから復号鍵を作成するステップと、

第２のデータを該復号鍵で復号するステップと、

復号の結果が所定の特徴を持つことを検査するステップとからなるデータ検証方法。

【請求項１９】　データ生成装置と、該生成装置で生成されたデータの真正性を検証するデータ検証装置とからなるデータ処理装置であって、

上記データ検証装置は

第１のデータを保持する基準値記憶部と、

第２のデータを保持する第１の副検査対象データ記憶部と、

上記第１の副検査対象データ記憶部に記憶されたデータから復号鍵を作成する復号鍵生成部と、

上記データ生成装置から送信されたデータを上記復号鍵生成部が生成した復号鍵で復号する復号部と、

上記復号部で復号されたデータが上記基準値記憶部に記憶されている上記第１のデータと所定の関係にあることを検査する検査部とからなり、

上記データ生成装置は、

上記データ検証装置から送付された上記第１のデータから第３のデータを作成する主検査対象データ生成部と、

第４のデータを保持する第２の副検査対象データ記憶部と、

上記第２の副検査対象データ記憶部に記憶されたデータから暗号鍵を作成する暗号鍵生成部と、

上記主検査対象データ生成部が作成した上記第３のデータを上記暗号鍵生成部

が生成した暗号鍵で暗号化する暗号部とからなり、

上記データ検証装置が、上記基準値記憶部に記憶されている上記第１のデータを上記データ生成装置に送信し、

上記データ生成装置が、上記主検査対象データ生成部で、上記データ検証装置から送信された上記第１のデータから上記第３のデータを生成し、さらに上記第３のデータを上記暗号部で暗号化して生成したデータを上記データ検証装置に送信し、

上記データ検証装置が、上記データ生成装置から送信されたデータを上記復号部で復号し、復号結果が上記基準値記憶部に記憶されている上記第１のデータと所定の関係にあることを上記検査部で検査することを特徴とするデータ処理装置。

【請求項２０】　上記データ生成装置が生成する上記第３のデータが、上記データ検証装置から送信された上記第１のデータを所定の復号鍵で復号したものであり、上記データ検証装置の上記検証部が、上記データ生成装置から送信されたデータの復号結果が、上記第１のデータに対する復号結果であることを検査することを特徴とする請求項１９記載のデータ処理装置。

【請求項２１】　上記データ生成装置が生成する上記第３のデータが、上記データ検証装置から送信された上記第１のデータに所定の署名鍵で署名して生成した署名値であり、上記データ検証装置の上記検証部が、上記データ生成装置から送信されたデータの復号結果が、上記基準値に対する正しい署名値であることを検査することを特徴とする請求項１９記載のデータ処理装置。

【請求項２２】　上記データ生成装置が、乱数値を保持する第１のコミットメント乱数記憶部と、コミットメント乱数値からコミットメント値を生成するコミットメント生成部とを更に備え、

上記データ検証装置が、上記データ生成装置から送信されたコミットメント値を記憶するコミットメント情報記憶部を更に備え、

上記データ生成装置が、上記データ検証装置から上記第１のデータを受け取る前に、上記コミットメント生成部が生成したコミットメント値を上記データ検証装置に送信し、

主検査対象生成部において被検証値である上記第３のデータを生成する際には、さらに、上記コミットメント乱数記憶部に記憶された乱数値も使用し、

上記データ検証装置が、上記検査部での検査の際に、上記コミットメント情報記憶部に記憶された上記コミットメント値も使用することを特徴とする請求項１９記載のデータ処理装置。

【請求項２３】　上記データ検証装置の上記復号鍵生成部が一方向性関数で構成されており、該一方向性関数に上記第１の副検査対象データ記憶部に記憶されたデータを入力して得られた結果が上記復号鍵であり、上記データ生成装置の上記暗号鍵生成部が上記データ検証装置の上記復号鍵生成部のものと同じ一方向性関数で構成されており、該一方向性関数に上記第２の副検査対象データ記憶部に記憶されたデータを入力して得られた結果が上記暗号鍵であることを特徴とする請求項１９記載のデータ処理装置。

【請求項２４】　上記データ検証装置が、

前鍵を保持する第１の前鍵保持部を更に備え、

上記復号鍵生成部が上記復号鍵を生成する際に、上記第１の前鍵保持部に記憶された上記前鍵も使用し、

上記データ作成装置が、

前鍵を保持する第２の前鍵保持部を更に備え、

上記暗号鍵生成部が上記暗号鍵を生成する際に、上記第２の前鍵保持部に記憶された上記前鍵も使用することを特徴とする請求項１９記載のデータ処理装置。

【請求項２５】　上記データ生成装置が、

上記前鍵を暗号化するための前鍵暗号鍵を保持する前鍵暗号鍵記憶部と、

上記前鍵暗号鍵記憶部に記憶された暗号鍵で上記前鍵を暗号化する前鍵暗号部とを備え、

上記データ検証装置が、

暗号化された上記前鍵を復号する前鍵復号鍵を記憶する前鍵復号鍵記憶部と、

上記前鍵復号鍵記憶部に記憶された上記前鍵復号鍵で暗号化された上記前鍵を復号する前鍵復号部とを備え、

上記データ生成装置が、上記前鍵を決定して、その前鍵を上記前鍵暗号鍵記憶

部に記憶された暗号鍵を使用して上記前鍵暗号部で暗号化し、その結果を上記データ検証装置に送信し、

上記データ検証装置が、上記データ生成装置から送信された暗号化された上記前鍵を上記前鍵復号鍵記憶部に記憶された上記前鍵復号鍵を使用して上記前鍵復号部で復号し、その結果を上記前鍵記憶部に記憶することを特徴とする請求項２４記載のデータ処理装置。

【請求項２６】　上記データ検証装置が、上記第１の副検査対象データ記憶部に保持されているデータを上記データ生成装置に送信し、

上記データ生成装置は、上記データ検証装置から送信された該データを上記第２の副検査対象データ記憶部に記憶して、上記暗号鍵の生成に使用することを特徴とする請求項１９記載のデータ処理装置。

【請求項２７】　上記データ生成装置が、上記第２の副検査対象データ記憶部に保持されているデータを上記データ検証装置に送信し、上記データ検証装置は、上記データ生成装置から送信された該データを上記第１の副検査対象データ記憶部に記憶して、上記復号鍵の生成に使用することを特徴とする請求項１９記載のデータ処理装置。

【請求項２８】　上記暗号部で行われる暗号化が、上記暗号鍵を鍵とした共通鍵暗号の暗号処理であり、上記復号部で行われる復号が、上記復号鍵を鍵とした共通鍵暗号の復号処理であることを特徴とする請求項１９記載のデータ処理装置。

【請求項２９】　上記暗号部で行われる暗号化が、所定の法数のもとでの第３のデータと上記暗号鍵の乗除算であり、上記復号部で行われる復号が、所定の法数のもとでの上記復号鍵と上記データ生成装置から送信されたデータの乗除算であることを特徴とする請求項１９記載のデータ処理装置。

【請求項３０】　第１のデータ記憶手段と暗号手段とを具備する第１の装置と、第２のデータ記憶手段と復号手段と検証手段とを具備する第２の装置とを有し、上記第１の装置は、上記第１のデータ記憶手段に記憶されているデータに基づいて所定の検証対象データを上記暗号手段により暗号化し、上記第２の装置は上記暗号化された上記所定の検証対象データを上記第２のデータ記憶手段に記憶

されているデータに基づいて上記復号手段により復号し、復号結果の真正性を上記検証手段で検証し、検証に成功した場合には上記第１のデータ記憶手段に記憶されているデータと上記第２のデータ記憶手段に記憶されているデータの同一性を認証することを特徴とするデータ処理装置。

【請求項３１】　上記第１のデータ記憶手段に記憶されているデータの少なくとも一部は上記第２の装置から送られてきたデータとする請求項３０記載のデータ処理装置。

【請求項３２】　上記第２のデータ記憶手段に記憶されているデータの少なくとも一部は上記第１の装置から送られてきたデータとする請求項３０または３１記載のデータ処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する利用分野】

この発明はデータ作成およびデータ検証技術に関し、とくに、データの暗号化・復号を行ないながらデータの検証手続を行う際にデータのやり取りを行うパーティ間のデータの真正性または同一性を簡易に検証できるようにしたものである。

【０００２】

【従来の技術】

メッセージの真正性（ｉｎｔｅｇｒｉｔｙ）を保証するための暗号学的な方法としては、メッセージ本体に、真正性チェック（ｉｎｔｅｇｒｉｔｙ　ｃｈｅｃｋ）用のデータを添付するものが知られている。添付されるデータはメッセージ認証コード（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ：ＭＡＣ）あるいはシール（ｓｅａｌ）と呼ばれる（以降ではＭＡＣに統一する）。

【０００３】

ＭＡＣを使用した真正性チェックの方法を以下に示す。

①メッセージの作者と受信者はともに、秘密の鍵ｋとシールを作成する際に使用するアルゴリズムＨ（）を共有している。

②メッセージの作成者は、メッセージｍからＭＡＣ、σ＝Ｈ（ｍ、ｋ）を作成し

、ｍにσを添付して受信者に送る。

③ＭＡＣσが添付されたメッセージｍを受け取った受信者は、Ｈ（ｍ、ｋ）がσと等しいかどうかを確認し、等しければメッセージの真正性が保たれていることがわかる。

【０００４】

上記の方法は、たとえば、「Ｗａｒｗｉｃｋ　Ｆｏｒｄ。　Ｃｏｍｐｕｔｅｒ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ　Ｓｅｃｕｒｉｔｙ、Ｐｒｅｎｔｉｃｅ　Ｈａｌｌ、１９９４、ｐｐ．７５－８０」に開示されている。

【０００５】

【発明が解決しようとする課題】

従来の技術では、ＭＡＣをメッセージに添付しなければならないために、送信されるデータ量がメッセージより増加してしまう。通常Ｈ（）にはＭＤ５（メッセージダイジェスト５）やＳＨＡ－１（セキュアーハッシュアルゴリズム）等の暗号学的ハッシュアルゴリズムが使用されるが、これによって作成されるＭＡＣは、ＭＤ５で１６ｂｙｔｅ、ＳＨＡ－１で２０ｂｙｔｅである。

【０００６】

メッセージ自体が文書のように大きかったり、通信速度の大きい環境下で通信する場合には、この増加はさほど問題にはならないが、少量のデータを低速度の通信環境で送信する場合には、無視できなくなる。

【０００７】

【課題を解決する手段】

ここで提案する発明は、メッセージが所定の特徴を持つデータを含んでいる場合に有効である。その特徴とは、そのデータが、受信者によってチェック可能な特定の条件を満たすことがわかっているというものである。

【０００８】

たとえば、そのデータが、特定のパターンの繰り返しといった冗長度を持つ場合や、そのデータがデジタル署名の署名値のように、特定の検証式を満たすことがわかっている場合がこれにあたる。

【０００９】

本発明のデータ生成装置は、所定の特徴を持つデータであって、その特徴を持つことが検証可能なデータである主検査対象データと、それ自身が特定の特徴を持つ必要がない（実際はなんらかの特徴を持つかもしれないが、別に持っていなくてもかまわない）副検査対象データを含むデータとを作成する。該データ生成装置は、データを暗号化する暗号部を持ち、主検査対象データを暗号部で暗号化する。暗号化のための鍵は、該データ生成装置が持つ暗号鍵生成部で、該データ生成装置内に保持されている副検査対象データから生成される。

【００１０】

上記のデータ生成装置によって生成されたデータの真正性の検証を行うデータ検証装置は、該データ生成装置の暗号鍵生成部と同じ鍵生成アルゴリズムを持つ復号鍵生成部を持っており、さらに被検証値が所定の特徴を持つことを検証する検証部を持つ。

【００１１】

このデータ検証装置は、データの検証の際に、副検査対象データから復号鍵を生成し、その鍵で暗号化された主検査対象データを復号し、復号結果が所定の特徴を持つことを検証する。

【００１２】

データ作成装置が、副検査対象データの一部をデータ検証装置が所持していることを知っている場合には、データ作成装置が所持する副検査対象データのすべてをデータ検証装置に送付する必要はない。

【００１３】

この検証に失敗した場合、以下のいずれかが起こっていることがデータ検証装置にわかる。

１．データ検証装置が持つ副検査対象データとデータ生成装置が持つ副検査対象データが異なっている。すなわち、副検査対象データの共有に失敗している。

２．たとえば、副検査対象データが検証者とデータ生成装置との間の送受信によって共有される場合には、送受信の過程でなんらかの差し替えが行われた可能性がある。

３．また、データ作成装置が、副検査対象データの一部をデータ検証装置が所持

していることを想定して、それを送付しなかった場合には、データ作成装置が想定しているのと同じデータをデータ検証装置が所持していない可能性がある。

４．データ生成装置自体が所定の特徴を持つ主検査対象データをつくることができない。たとえば、所定の特徴を持つ主検査対象データを作れるのが、特定の情報を持つものに限られている場合、データ生成装置はその範疇に該当しない。

【００１４】

この方式によれば、データ生成装置が生成するデータには、真正性保証のためのＭＡＣに当たる情報は、暗号化された主検査対象データに畳み込まれており、ＭＡＣをデータに添付する必要性をなくしている。

【００１５】

本発明で用いる暗号鍵生成部あるいは復号鍵生成部は、一方向性関数で構成するのが一般的である。

【００１６】

ＭＤ５あるいはＳＨＡ－１等のアルゴリズムが公開された一方向性ハッシュ関数を使用した場合、本発明のデータ生成装置が作成したデータについては、故意に改竄行為がなされた可能性を除いて、データに問題がないことが保証できる。

【００１７】

もし、非公開の一方向性関数を使用した場合には、データがその非公開の一方向性関数を所持しているデータ作成装置で生成されたものであるかどうかを検査できる。すなわち、非公開の一方向性関数を共有している者以外による故意の改竄を排除できる。ただし、検査ができるのは、同じ非公開の一方向性関数を共有しているデータ検証装置のみである。

【００１８】

また、この構成をとった場合の付加的な利点として、非公開の一方向性関数を共有しているもの以外には、主検査対象データを秘密にできるということがある。

【００１９】

データ作成装置とデータ検証装置が秘密のデータ（前鍵と呼ぶ）を共有し、暗号鍵生成や復号鍵生成の際にその前鍵を使用することでも、同様の効果を得るこ

とができる。

【００２０】

この方法でも、検査ができるのは、同じ前鍵を共有しているデータ検証装置のみであるが、データ作成装置からデータ検証装置に前鍵を送ることで、任意のデータ検証装置にデータの検査を行わせることが可能になる。当然、前鍵は暗号化されたデータ検証装置に送付されなければならないが、その暗号に公開鍵暗号をもちいれば、暗号鍵が公開されているどのデータ検証装置にもデータの検証を実行させることができる。

【００２１】

本発明をさらに詳細に説明する。

【００２２】

本発明によれば、データの真正性を低コストに検証するために、データ生成装置と、該生成装置で生成されたデータの真正性を検証するデータ検証装置とからなるデータ処理装置を構成する。そして、上記データ検証装置には、第１のデータを保持する基準値記憶部と、第２のデータを保持する第１の副検査対象データ記憶部と、上記第１の副検査対象データ記憶部に記憶されたデータから復号鍵を作成する復号鍵生成部と、上記データ生成装置から送信されたデータを上記復号鍵生成部が生成した復号鍵で復号する復号部と、上記復号部で復号されたデータが上記基準値記憶部に記憶されている上記第１のデータと所定の関係にあることを検査する検査部とを設ける。上記データ生成装置には、上記データ検証装置から送付された上記第１のデータから第３のデータを作成する主検査対象データ生成部と、第４のデータを保持する第２の副検査対象データ記憶部と、上記第２の副検査対象データ記憶部に記憶されたデータから暗号鍵を作成する暗号鍵生成部と、上記主検査対象データ生成部が作成した上記第３のデータを上記暗号鍵生成部が生成した暗号鍵で暗号化する暗号部とを設ける。上記データ検証装置が、上記基準値記憶部に記憶されている上記第１のデータを上記データ生成装置に送信し、上記データ生成装置が、上記主検査対象データ生成部で、上記データ検証装置から送信された上記第１のデータから上記第３のデータを生成し、さらに上記第３のデータを上記暗号部で暗号化して生成したデータを上記データ検証装置に

送信し、上記データ検証装置が、上記データ生成装置から送信されたデータを上記復号部で復号し、復号結果が上記基準値記憶部に記憶されている上記第１のデータと所定の関係にあることを上記検査部で検査する。

【００２３】

この構成においては、主検査対象データの検証を行いつつ、その検証手続に上記副検査対象データを畳み込んでいるので、副検査対象データの検証を別途行う必要がなく、また、ＭＡＣ等を付加する必要もない。

【００２４】

なお、データ生成装置が生成するデータは、暗号部による暗号化結果および第２の副検査対象データ記憶部の記憶内容の双方を同時に含むデータでもよい。あるいは、データ生成装置が、暗号部による暗号化結果を含むデータと、第２の副検査対象データ記憶部の記憶内容を含むデータとを、個別のタイミングで生成して、これらが別々のタイミングでデータ検証装置に送られるようにしてもよい。

【００２５】

また、副検査対象データはどちらから送信するようにしてもよく、また、データ生成装置およびデータ検証装置の双方に第３者から送られたものでもよい。また、データのソースが一部はデータ生成装置、一部はデータ検証装置また一部はそれ以外であるような場合も適用できる。

【００２６】

また、この構成において、上記データ生成装置が生成する上記第３のデータが、上記データ検証装置から送信された上記第１のデータを所定の復号鍵で復号したものであり、上記データ検証装置の上記検証部が、上記データ生成装置から送信されたデータの復号結果が、上記第１のデータに対する復号結果であることを検査するようにしてもよい。

【００２７】

また、上記データ生成装置が生成する上記第３のデータが、上記データ検証装置から送信された上記第１のデータに所定の署名鍵で署名して生成した署名値であり、上記データ検証装置の上記検証部が、上記データ生成装置から送信されたデータの復号結果が、上記基準値に対する正しい署名値であることを検査するよ

うにしてもよい。

【００２８】

また、上記データ生成装置が、乱数値を保持する第１のコミットメント乱数記憶部と、コミットメント乱数からコミットメント値を生成するコミットメント生成部とを更に備え、上記データ検証装置が、上記データ生成装置から送信されたコミットメント値を記憶するコミットメント情報記憶部を更に備え、上記データ生成装置が、上記データ検証装置から上記第１のデータを受け取る前に、上記コミットメント生成部が生成したコミットメント値を上記データ検証装置に送信し、主検査対象生成部において被検証値である上記第３のデータを生成する際には、さらに、上記コミットメント乱数記憶部に記憶された乱数値も使用し、上記データ検証装置が、上記検査部での検査の際に、上記コミットメント情報記憶部に記憶された上記コミットメント値も使用するようにしてもよい。

【００２９】

また、上記データ検証装置の上記復号鍵生成部が一方向性関数で構成されており、該一方向性関数に上記第１の副検査対象データ記憶部に記憶されたデータを入力して得られた結果が上記復号鍵であり、上記データ生成装置の上記暗号鍵生成部が上記データ検証装置の上記復号鍵生成部のものと同じ一方向性関数で構成されており、該一方向性関数に上記第２の副検査対象データ記憶部に記憶されたデータを入力して得られた結果が上記暗号鍵であるようにしてもよい。

【００３０】

また、上記データ検証装置が、前鍵を保持する第１の前鍵保持部を更に備え、上記復号鍵生成部が上記復号鍵を生成する際に、上記第１の前鍵保持部に記憶された上記前鍵も使用し、上記データ作成装置が、前鍵を保持する第２の前鍵保持部を更に備え、上記暗号鍵生成部が上記暗号鍵を生成する際に、上記第２の前鍵保持部に記憶された上記前鍵も使用するようにしてもよい。

【００３１】

また、上記データ生成装置が、上記前鍵を暗号化するための前鍵暗号鍵を保持する前鍵暗号鍵記憶部と、上記前鍵暗号鍵記憶部に記憶された暗号鍵で上記前鍵を暗号化する前鍵暗号部とを備え、上記データ検証装置が、暗号化された上記前

鍵を復号する前鍵復号鍵を記憶する前鍵復号鍵記憶部と、上記前鍵復号鍵記憶部に記憶された上記前鍵復号鍵で暗号化された上記前鍵を復号する前鍵復号部とを備え、上記データ生成装置が、上記前鍵を決定して、その前鍵を上記前鍵暗号鍵記憶部に記憶された暗号鍵を使用して上記前鍵暗号部で暗号化し、その結果を上記データ検証装置に送信し、上記データ検証装置が、上記データ生成装置から送信された暗号化された上記前鍵を上記前鍵復号鍵記憶部に記憶された上記前鍵復号鍵を使用して上記前鍵復号部で復号し、その結果を上記前鍵記憶部に記憶するようにしてもよい。

【００３２】

また、上記データ検証装置が、上記第１の副検査対象データ記憶部に保持されているデータを上記データ生成装置に送信し、上記データ生成装置は、上記データ検証装置から送信された該データを上記第２の副検査対象データ記憶部に記憶して、上記暗号鍵の生成に使用するようにしてもよい。

【００３３】

また、上記データ生成装置が、上記第２の副検査対象データ記憶部に保持されているデータを上記データ検証装置に送信し、上記データ検証装置は、上記データ生成装置から送信された該データを上記第１の副検査対象データ記憶部に記憶して、上記復号鍵の生成に使用するようにしてもよい。

【００３４】

また、上記暗号部で行われる暗号化が、上記暗号鍵を鍵とした共通鍵暗号の暗号処理であり、上記復号部で行われる復号が、上記復号鍵を鍵とした共通鍵暗号の復号処理であるようにしてもよい。

【００３５】

また、上記暗号部で行われる暗号化が、所定の法数のもとでの第３のデータと上記暗号鍵の乗除算であり、上記復号部で行われる復号が、所定の法数のもとでの上記復号鍵と上記データ生成装置から送信されたデータの乗除算であるようにしてもよい。

【００３６】

なお、本発明は、データ生成装置やデータ検証装置としても実現でき、またそ

れらの方法としても実現できる。また本発明の少なくとも一部をコンピュータプログラム製品として実現することもできる。

【００３７】

【発明の実施の態様】

以下、この発明の実施例について説明する。

【００３８】

［第１の実施例］

図１は、本発明を適用した第１の実施例の構成図である。

【００３９】

本実施例は、データを生成するデータ生成器１００と、データ生成器１００で生成されたデータの正当性を検証するデータ検証器２００からなるシステムである。データ生成器１００とデータ検証器２００の間ではデータの送受信が行われる。送受信はインターネット経由、イントラネット経由、電話回線経由、同一計算機内でのプロセス間通信等、種々の方法が可能である。　基本的な機能は、データ検証器２００が送付したデータに対してデータ生成器１００が署名値を計算し、データ検証器２００に送り返すものである。

【００４０】

また、このデータ送受信の過程で、データ検証器２００からデータ生成器１００への情報の送付、およびその逆方向の情報の送付も行うことができる。具体的には、署名を依頼した日時情報をデータ検証器２００からデータ生成器１００に送付することができるし、署名を生成したデータ生成器１００の識別子をデータ生成器１００からデータ検証器２００に送ることができる。

【００４１】

この過程で、データ検証器２００は、自分が送付した情報が改ざんされることなくデータ生成器１００に届いたこと、情報を送付してきたデータ生成器１００が署名を作成したデータ生成器１００と同一であり、そのデータに改ざんが施されていないことを確認できる。

【００４２】

データ生成器１００が含むモジュールの役割について以下に記す。

［受信部１０１］：データ検証器２００から送付されたデータを受け取り、通信用フォーマットからデータ生成器１００内部のフォーマットに変換した後、受信したデータをデータ生成器１００内のほかのモジュールに振り分ける。

［送信部１０２］：データ生成器１００の各モジュールから受け取ったデータを通信に適したフォーマットに変換しデータ検証器２００に送付する。

［署名生成部１０３］：受信部１０１経由でデータ検証器２００から送付された被署名値（署名の対象となるデータ）に対する署名値を作成するモジュールである。本実施例でデータ生成器１００が作成する署名は、データ検証器２００から送信された被署名値にＳＨＡ－１を適用した結果にＲＳＡ（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｌｅｍａｎ）署名を施したものである。署名生成部１０３は、ＳＨＡ－１のハッシュを実行するプログラムと、ＲＳＡの署名鍵を内蔵している。

［暗号部１０４］：署名生成部１０３で生成された署名値を暗号化するモジュールである。このモジュールで行う暗号化は、データ検証部２００の暗号文復号部２０４が復号に使用するのと同じＲＳＡ法数のもとでの、鍵生成部１０５で生成される鍵と署名生成部１０３が生成した署名値との剰余演算である。

［鍵生成部１０５］：暗号部１０４で使用される暗号鍵を生成するモジュールである。このモジュールはＳＨＡ－１等のハッシュ関数で構成されている。後述する前鍵記憶部１０６に記憶されている前鍵と、鍵生成用データ記憶部１０９に記憶されているデータに、このハッシュ関数を適用した結果が鍵となる。

［前鍵生成部１０６］：鍵生成部１０５での鍵の生成に使用される前鍵を生成するモジュールである。生成する前鍵を攻撃者に予測されないよう、乱数生成器等を使って前鍵を生成する。

【００４３】

前鍵は、データ検証器２００に送られ、データ生成器１００とデータ検証器２００の間で共有される。共有されている間は、データ検証器２００に前鍵を送る必要はない。いつ共有をやめて、新しい前鍵をデータ検証器２００に送るかは前鍵生成部１０６が決定する。そのため前鍵生成部１０６は、時計を内蔵しており、以前前鍵を送付してから一定時間が過ぎると、新たな前鍵を生成する。

［前鍵暗号部１０７］：前鍵を暗号化し、その結果を送信部１０２に送るモジュ

ールである。このモジュールでの暗号化はＲＳＡ暗号を用いる。このモジュールはＲＳＡ暗号を実施するプログラムと、暗号鍵を内蔵している。

［前鍵記憶部１０８］：前鍵生成部１０６が作成した前鍵を記憶するモジュールである。このモジュールが記憶している前鍵は、鍵生成部１０５が鍵を生成する際、および、前鍵暗号部１０７が前鍵を暗号化する際に参照される。

［鍵生成用データ記憶部１０９］：鍵生成部１０５での鍵の生成に使用されるデータを記憶しているモジュールである。具体的には、署名依頼日時の情報と、このデータ生成器１００の識別子を記憶している。前者のデータは、データ検証器２００から送信されるものである。後者のデータは、本データ生成器１００に埋め込まれたものであり、送信部１０２を通して、データ検証器２００に送信される。

【００４４】

データ検証器２００が含むモジュールの役割について以下に記す。

［送信部２０１］：データを通信に適したフォーマットに変換しデータ生成器１００に送付する。

［受信部２０２］：データ生成器１００から送付されたデータを受け取り、通信用フォーマットからデータ検証器２００内部のフォーマットに変換した後、受信したデータをデータ検証器２００内のほかのモジュールに振り分ける。

［被署名値記憶部２０３］：このモジュールにデータ生成器１００に署名を依頼するデータが記憶されている。ここに記憶されているデータは、送信部２０１を通してデータ生成器１００に送られる。また、署名検証部２０５が署名値を検証する際に参照される。

［復号部２０４］：データ生成器１００から送信されたデータに含まれる暗号化された署名値を復号するモジュールである。ここで行われる復号は、署名検証部２０５での署名値の検証に使われるＲＳＡ法数のもとで、暗号化された署名値を鍵生成部２０６で生成される鍵で割る演算である。

［署名検証部２０５］：復号部２０４で復号した署名値の正当性を検証するモジュールである。このモジュールは、ＳＨＡ－１を実行するプログラムと、データ生成器１００の署名生成部１０３が所持する署名鍵に対応する検証鍵を内蔵して

いる。被署名値記憶部２０３に記憶されているデータにＳＨＡ－１を適用した結果が署名値を検証鍵でべき乗剰余した結果と同一かどうかで、署名値の正当性を検証する。

［鍵生成部２０６］：復号部２０４が使用する復号鍵を作成するモジュールである。データ生成器１００の鍵生成部１０５が持つのと同じハッシュ関数で構成されている。後述する前鍵記憶部２０７に記憶されている前鍵と、鍵生成用データ記憶部２０９に記憶されているデータに、このハッシュ関数を適用した結果が鍵となる。

［前鍵記憶部２０７］：前鍵復号部２０８が復号した前鍵を記憶するモジュールである。このモジュールが記憶している前鍵は、鍵生成部２０６が鍵を生成する際に参照される。

［前鍵復号部２０８］：前鍵は暗号化された状態でデータ生成器１００から送信される。このモジュールは、暗号化された前鍵を復号する。このモジュールでの復号にはＲＳＡ復号を用いる。その復号鍵は、データ生成器１００の前鍵暗号部１０７が保持する暗号鍵に対応する復号鍵であり、本モジュールはこの復号鍵を内蔵している。

［鍵生成用データ記憶部２０９］：鍵生成部２０６での鍵の生成に使用されるデータを記憶しているモジュールである。具体的には、署名依頼日時の情報と、署名を生成したデータ生成器１００の識別子を記憶している。前者のデータは、本データ検証器２００に付随したクロックから取り出される。後者のデータは、データ生成器１００から署名値とともに送信される。

【００４５】

本実施例の動作について説明する。

【００４６】

本実施例は、大まかには、データ検証器２００がデータ生成器１００に被署名値を含むデータ（署名作成依頼と呼ぶ）を送付し、データ生成器１００がデータ検証器２００に署名値を含むデータ（署名データと呼ぶ）を返信し、データ検証器２００で署名データの正当性を検査するというステップを踏む。

【００４７】

データ検証器２００が署名作成依頼を作成するときの動作を以下に示す。なお、この手順自体は簡潔なのでとくに図示しない。

［前提］：被署名データが被署名値記憶部２０３に記憶されている状態からスタートする。

［ステップ１］：データ検証器２００が内蔵している時計から現在時刻情報を取り出し、それを署名依頼時刻として鍵生成用データ記憶部１０９に記憶する。

［ステップ２］：被署名値記憶部２０３に記憶されている被署名値と、鍵生成用データ記憶部２０９に記憶されている署名依頼時刻とから署名作成依頼を作成し、送信部２０１からデータ生成器１００に送付する。

【００４８】

署名作成依頼を受け取ったデータ生成器１００の動作を以下に示すに示す。また、この動作の手順を記述したフローチャートを図２に示す。

［ステップＳ１０１］：　受信部１０１で受信した署名作成依頼から、署名依頼時刻を取り出し、鍵生成用データ記憶部１０９に記憶する。

［ステップＳ１０２］：受信部１０１で受信した署名作成依頼から、被署名値を取り出して署名生成部１０３に送付し、署名生成部１０３で、被署名値に対する署名値を作成する。

［ステップＳ１０３］：もし、新しい前鍵の生成が必要なら、前鍵生成部１０６で前鍵を作成し、前鍵記憶部１０８に記憶する。必要でなければ、ステップＳ１０５へ進む。

［ステップＳ１０４］：前鍵暗号部１０７で前鍵記憶部１０８に記憶されている前鍵を暗号化する。

［ステップＳ１０５］：鍵生成部１０５で、前鍵記憶部１０８に記憶されている前鍵と、鍵生成用データ記憶部１０９に記憶されている署名依頼日時と本データ生成器１００の識別子から、鍵を生成する。

［ステップＳ１０６］：署名生成部１０３で生成された署名値を、鍵生成部１０５で生成された鍵を用い、暗号部１０４で暗号化する。

［ステップＳ１０７］：暗号部１０４で暗号化された署名値と、もしあれば前鍵暗号部１０７で暗号化された前鍵と、鍵生成用データ記憶部１０９に記憶されて

いる本データ生成器１００の識別子とから署名データを作成し、送信部１０２からデータ検証器２００に送付する。

【００４９】

署名データを受け取ったデータ検証器２００の動作を以下に示す。また、この動作の手順を記述したフローチャートを図３に示す。

【００５０】

［ステップＳ１１１］：受信部２０２で受信した署名データから、署名を生成したデータ生成器１００の識別子を取り出し、鍵生成用データ記憶部２０９に記憶する。

［ステップＳ１１２］：署名データに暗号化された前鍵が含まれていれば、それを取り出し、前鍵復号部２０８で復号し、その結果を前鍵記憶部２０７に記憶する。もし、暗号化された前鍵が含まれていなければ、何もせずステップＳ１１３へ進む。

［ステップＳ１１３］：鍵生成部２０６で、前鍵記憶部２０７に記憶されている前鍵と、鍵生成用データ記憶部２０９に記憶されている署名依頼日時とデータ生成器１００の識別子から、鍵を生成する。

［ステップＳ１１４］：署名データから暗号化された署名値を取り出し、鍵生成部２０６で生成された鍵を使用して、復号部２０４で復号する。

［ステップＳ１１５］：復号部２０４での復号の結果が、被署名値記憶部２０３に記憶されている被署名値の正しい署名であるかどうかを署名検証部２０５で検査する。

【００５１】

データ検証器２００が、ステップＳ１１５の検査で、正しい署名値であることが確認できた場合、データ検証器２００にとっては、以下のことが保証される。

【００５２】

１．データ生成器１００が作成した署名値が、被署名値に対して正しい署名であること。

２．データ検証器２００が送付した署名依頼日時が、差し替えられることなくデータ生成器１００に届いたこと。

３．受け取ったデータ生成器１００の識別子が、署名を生成したデータ生成器１００と同一のものであること。

【００５３】

［第２の実施例］

図４は、本発明を適用した第２の実施例の構成図である。

【００５４】

本実施例は、第１の実施例と同様に、データを生成するデータ生成器１００と、データ生成器１００で生成されたデータの正当性を検証するデータ検証器２００からなるシステムである。データ生成器１００とデータ検証器２００の間ではデータの送受信が行われる。送受信はインターネット経由、イントラネット経由、電話回線経由、同一計算機内でのプロセス間通信等、種々の方法が可能である。

【００５５】

基本的な機能は、データ検証器２００が送付した暗号文をデータ生成器１００が復号し、その結果をデータ検証器２００に送り返すものである。

【００５６】

また、このデータ送受信の過程で、データ検証器２００からデータ生成器１００への情報の送付、およびその逆方向の情報の送付も行うことができる。具体的には、復号を依頼した日時情報をデータ検証器２００からデータ生成器１００に送付することができるし、復号を実行したデータ生成器１００の識別子をデータ生成器１００からデータ検証器２００に送ることができる。

【００５７】

この過程で、データ検証器２００は、自分が送付した情報が改ざんされることなくデータ生成器１００に届いたこと、情報を送付してきたデータ生成器１００が復号を行ったデータ生成器１００と同一であり、そのデータに改ざんが施されていないことを確認できる。

【００５８】

データ生成器１００が含むモジュールの役割について以下に記す。

［受信部１０１］：データ検証器２００から送付されたデータを受け取り、通信

用フォーマットからデータ生成器１００内部のフォーマットに変換した後、受信したデータをデータ生成器１００内のほかのモジュールに振り分ける。

［送信部１０２］：データ生成器１００の各モジュールから受け取ったデータを通信に適したフォーマットに変換しデータ検証器２００に送付する。

［暗号文復号部１１０］：受信部１０１経由でデータ検証器２００から送付された暗号文を復号するモジュールである。本実施例でデータ生成器１００が採用する復号アルゴリズムはＲＳＡである。このモジュールは、ＲＳＡの復号鍵を内蔵している。

［暗号部１０４］：暗号文復号部１１０で生成された復号結果を暗号化するモジュールである。このモジュールで行われる暗号はＤＥＳ－ＣＢＣ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ－Ｃｉｐｈｅｒ Ｂｌｏｃｋ Ｃｈａｉｎｉｎｇ ｍｏｄｅ）である。このモジュールはＤＥＳ－ＣＢＣを実行できるプログラムを内蔵している。

［鍵生成部１０５］：暗号部１０４で使用される暗号鍵を生成するモジュールである。ここで生成される暗号鍵は、暗号部１０４で使用されるＤＥＳ－ＣＢＣの初期ベクタ６４ｂｉｔと暗号鍵５６ｂｉｔのあわせて１２０ｂｉｔのデータである。このデータは、後述する前鍵記憶部１０８に記憶されている前鍵と、鍵生成用データ記憶部１０９に記憶されているデータに１２０ｂｉｔのハッシュ値を出力する一方向性関数を施した結果である。したがって、このモジュールは１２０ｂｉｔのハッシュ値を出力する一方向性関数を実行するプログラムを内蔵している。

［前鍵生成部１０６］：鍵生成部１０５での鍵の生成に使用される前鍵を生成するモジュールである。生成する前鍵を攻撃者に予測されないよう、乱数生成器等を使って前鍵を生成する。

【００５９】

前鍵は、データ検証器２００に送られ、データ生成器１００とデータ検証器２００の間で共有される。共有されている間は、データ検証器２００に前鍵を送る必要はない。いつ共有をやめて、新しい前鍵をデータ検証器２００に送るかは前鍵生成部１０６が決定する。そのため前鍵生成部１０６は、時計を内蔵しており

、以前前鍵を送付してから一定時間が過ぎると、新たな前鍵を生成する。

［前鍵暗号部１０７］：前鍵を暗号化し、その結果を送信部１０２に送るモジュールである。このモジュールでの暗号化はＲＳＡ暗号を用いる。このモジュールはＲＳＡ暗号を実施するプログラムと、暗号鍵を内蔵している。

［前鍵記憶部１０８］：前鍵生成部１０６が作成した前鍵を記憶するモジュールである。このモジュールが記憶している前鍵は、鍵生成部１０５が鍵を生成する際、および、前鍵暗号部１０７が前鍵を暗号化する際に参照される。

［鍵生成用データ記憶部１０９］：鍵生成部１０５での鍵の生成に使用されるデータを記憶しているモジュールである。具体的には、署名依頼日時の情報と、このデータ生成器１００の識別子を記憶している。前者のデータは、データ検証器２００から送信されるものである。後者のデータは、本データ生成器１００に埋め込まれたものであり、送信部１０２を通して、データ検証器２００に送信される。

【００６０】

データ検証器２００が含むモジュールの役割について以下に記す。

［送信部２０１］：データを通信に適したフォーマットに変換しデータ生成器１００に送付する。

［受信部２０２］：データ生成器１００から送付されたデータを受け取り、通信用フォーマットからデータ検証器２００内部のフォーマットに変換した後、受信したデータをデータ検証器２００内のほかのモジュールに振り分ける。

［暗号文記憶部２１０］：このモジュールにデータ生成器１００に復号を依頼する暗号文が記憶されている。ここに記憶されているデータは、送信部２０１を通してデータ生成器１００に送られる。ここに蓄積されているデータは、特定のフォーマットを持つ平文をＲＳＡで暗号化したものであり、その暗号鍵は、データ生成器１００の暗号文復号部１１０が内蔵する復号鍵に対応するものである。

［復号部２０４］：データ生成器１００から送信されたデータに含まれる暗号化されたデータを復号するモジュールである。ここで行われる復号は、ＤＥＳ－ＣＢＣであり、このモジュールはＤＥＳ－ＣＢＣを実行するプログラムを内蔵している。

［復号結果検証部２１１］：復号部２０４で復号したデータが、データ生成器１００に復号を依頼した暗号文の復号結果であることを検査するモジュールである。データが所定のフォーマットをしていれば、それを正当なものであると判定する。

［鍵生成部２０６］：復号部２０４が使用する復号鍵を作成するモジュールである。ここで生成される鍵は、復号部２０４で使用されるＤＥＳ－ＣＢＣの初期ベクタ６４ｂｉｔと復号鍵５６ｂｉｔのあわせて１２０ｂｉｔのデータである。このデータは、後述する前鍵記憶部２０７に記憶されている前鍵と、鍵生成用データ記憶部２０９に記憶されているデータに、データ生成器１００の鍵生成部１０５が持つのと同じ１２０ｂｉｔのハッシュ値を出力する一方向性関数を施した結果である。したがって、このモジュールは１２０ｂｉｔのハッシュ値を出力するデータ生成器１００の鍵生成部１０５が持つのと同じ一方向性関数を実行するプログラムを内蔵している。

［前鍵記憶部２０７］：前鍵復号部２０８が復号した前鍵を記憶するモジュールである。このモジュールが記憶している前鍵は、鍵生成部２０６が鍵を生成する際に参照される。

［前鍵復号部２０８］：前鍵は暗号化された状態でデータ生成器１００から送信される。このモジュールは、暗号化された前鍵を復号する。このモジュールでの復号にはＲＳＡ復号を用いる。その復号鍵は、データ生成器１００の前鍵暗号部１０７が保持する暗号鍵に対応する復号鍵であり、本モジュールはこの復号鍵を内蔵している。

［鍵生成用データ記憶部２０９］：鍵生成部２０６での鍵の生成に使用されるデータを記憶しているモジュールである。具体的には、署名依頼日時の情報と、署名を生成したデータ生成器１００の識別子を記憶している。前者のデータは、本データ検証器２００に付随したクロックから取り出される。後者のデータは、データ生成器１００から暗号文とともに送信される。

【００６１】

本実施例の動作について説明する。

【００６２】

本実施例は、大まかには、データ検証器２００がデータ生成器１００に暗号文を含むデータ（復号依頼と呼ぶ）を送付し、データ生成器１００がデータ検証器２００に復号結果を含むデータ（復号データと呼ぶ）を返信し、データ検証器２００で復号データの正当性を検査するというステップを踏む。

【００６３】

データ検証器２００が復号依頼を作成するときの動作を以下に示す。なお、復号依頼の手順自体は簡潔であるので図示しない。

［前提］：暗号文が暗号文記憶部２１０に記憶されている状態からスタートする。

［ステップ１］：データ検証器２００が内蔵している時計から現在時刻情報を取り出し、それを復号依頼時刻として鍵生成用データ記憶部２０９に記憶する。

［ステップ２］：暗号文記憶部２１０に記憶されている暗号文と、鍵生成用データ記憶部２０９に記憶されている復号依頼時刻とから復号依頼を作成し、送信部２０１からデータ生成器１００に送付する。

【００６４】

復号依頼を受け取ったデータ生成器１００の動作を以下に示すに示す。また、この動作の手順を記述したフローチャートを図５に示す。

【００６５】

［ステップＳ１２１］：受信部１０１で受信した復号依頼から、復号依頼時刻を取り出し、鍵生成用データ記憶部１０９に記憶する。

［ステップＳ１２２］：受信部１０１で受信した復号依頼から、暗号文を取り出して暗号文復号部１１０に送付し、暗号文復号部１１０で、暗号文を復号する。

［ステップＳ１２３］：もし、新しい前鍵の生成が必要なら、前鍵生成部１０６で前鍵を作成し、前鍵記憶部１０８に記憶する。必要でなければ、ステップＳ１２５へ進む。

［ステップＳ１２４］：前鍵暗号部１０７で前鍵記憶部１０８に記憶されている前鍵を暗号化する。

［ステップＳ１２５］：鍵生成部１０５で、前鍵記憶部１０８に記憶されている前鍵と、鍵生成用データ記憶部１０９に記憶されている復号依頼日時と本データ

生成器１００の識別子から、鍵を生成する。

［ステップＳ１２６］：暗号文復号部１１０での復号結果を、鍵生成部１０５で生成された鍵を用いて、暗号部１０４で暗号化する。

［ステップＳ１２７］：暗号部１０４で暗号化された復号結果と、もしあれば前鍵暗号部１０７で暗号化された前鍵と、鍵生成用データ記憶部１０９に記憶されている本データ生成器１００の識別子とから復号データを作成し、送信部１０２からデータ検証器２００に送付する。

【００６６】

復号データを受け取ったデータ検証器２００の動作を以下に示す。また、この動作の手順を記述したフローチャートを図６に示す。

【００６７】

［ステップＳ１３１］：受信部２０２で受信した復号データから、復号を実行したデータ生成器１００の識別子を取り出し、鍵生成用データ記憶部２０９に記憶する。

［ステップＳ１３２］：復号データに暗号化された前鍵が含まれていれば、それを取り出し、前鍵復号部２０８で復号し、その結果を前鍵記憶部２０７に記憶する。もし、暗号化された前鍵が含まれていなければ、何もせずステップＳ１３３へ進む。

［ステップＳ１３３］：鍵生成部２０６で、前鍵記憶部２０７に記憶されている前鍵と、鍵生成用データ記憶部２０９に記憶されている復号依頼日時とデータ生成器の識別子から、鍵を生成する。

［ステップＳ１３４］：復号データから暗号化された復号結果を取り出し、鍵生成部２０６で生成された鍵を使用して、復号部２０４で復号する。

［ステップＳ１３５］：復号部２０４での復号の結果が、所定のフォーマットのデータであるかどうかを復号結果検証部２１１で検査する。

【００６８】

データ検証器２００が、ステップＳ１３５の検査で、復号結果が所定のフォーマットを満たしていることが確認できた場合、データ検証器２００にとっては、以下のことが保証される。

【００６９】

１．データ生成器１００が作成した復号結果が正しいこと。

２．データ検証器２００が送付した復号依頼日時が、差し替えられることなくデータ生成器１００に届いたこと。

３．受け取ったデータ生成器１００の識別子が、復号を実行したデータ生成器１００と同一のものであること。

【００７０】

なお、本実施例における所定のフォーマットまたはパターンとはどのようなものでもよい。実際の文書のパターンをも利用できる。例えば、文書のうち規則性のある部分を主検査対象データとし、その他の部分を副検査対象データとする。図１０に示すようなＨＴＭＬ（Ｈｙｐｅｒｔｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）文書においてはヘッダ部分を主検査対象データとし、ボディ部分を副検査対象データとして、主検査対象データのヘッダ部分の特徴を検査することにより、データ生成器およびデータ検証器のデータの同一性を検証できる。この場合、ヘッダ部分またはそれを含む部分を暗号化してデータ生成器に送り、その他の部分を、そのまま共有したいデータとして送り、あるいは送られることにより、効率のよいデータの共有化を保証できる。

【００７１】

また、ＨＴＭＬ文書の他、他のＳＧＭＬ（Ｓｔａｎｄａｒｄ　Ｇｅｎｅｒａｌｉｚｅｄ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）文書、例えばＸＭＬ（Ｅｘｔｅｎｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）やそのスタイルシートにも適用できる。

【００７２】

また、主検査対象データの特徴としては文字列自体を採用してもよい。すなわち、主検査対象データに含まれる所定の文字列があるかどうかを検証してもよい。

【００７３】

［第３の実施例］

図７は、本発明を適用した第３の実施例の構成図である。

【００７４】

本実施例は、データを生成するデータ生成器１００と、データ生成器１００で生成されたデータの正当性を検証するデータ検証器２００からなるシステムである。データ生成器１００とデータ検証器２００の間ではデータの送受信が行われる。送受信はインターネット経由、イントラネット経由、電話回線経由、同一計算機内でのプロセス間通信等、種々の方法が可能である。

【００７５】

基本的な機能は、データ検証器２００がデータ生成器１００を認証することであり、データ生成器１００がコミットメントを作成してデータ検証器２００に送付し、データ検証器２００がチャレンジをデータ生成器１００に送付し、チャレンジに対するレスポンスをデータ生成器１００が計算し、データ検証器２００に送り返すものである。

【００７６】

また、このデータ送受信の過程で、データ検証器２００からデータ生成器１００への情報の送付、およびその逆方向の情報の送付も行うことができる。具体的には、認証を実行した日時情報をデータ検証器２００からデータ生成器１００に送付することができるし、レスポンスを生成したデータ生成器１００の識別子をデータ生成器１００からデータ検証器２００に送ることができる。

【００７７】

この過程で、データ検証器２００は、自分が送付した情報が改ざんされることなくデータ生成器１００に届いたこと、情報を送付してきたデータ生成器１００が証明を行ったデータ生成器１００と同一であり、そのデータに改ざんが施されていないことを確認できる。

【００７８】

データ生成器１００が含むモジュールの役割について以下に記す。

［受信部１０１］：データ検証器１００から送付されたデータを受け取り、通信用フォーマットからデータ生成器１００内部のフォーマットに変換した後、受信したデータをデータ生成器１００内のほかのモジュールに振り分ける。

［送信部１０２］：データ生成器１００の各モジュールから受け取ったデータを

通信に適したフォーマットに変換しデータ検証器２００に送付する。

［乱数生成部１２０］：コミットメントのもととなる乱数を生成するモジュールである。

［乱数記憶部１２１］：乱数生成部１２０で生成された乱数を記憶するモジュールである。

［コミットメント生成部１２２］：乱数記憶部１２１に記憶されている乱数をもとに、コミットメントを生成するモジュールである。

［レスポンス生成部１２３］：受信部１０１経由でデータ検証器２００から送付されたチャレンジに対するレスポンスを作成するモジュールである。本実施例でデータ生成器はＧｕｉｌｌｏｕ－Ｑｕｉｓｑｕａｔｅｒ認証方式に基づいてレスポンスを生成する。レスポンス生成の際には、チャレンジだけでなく、乱数記憶部１２１に記憶されている乱数も使用される。

［暗号部１０４］：レスポンス生成部１２３で生成されたレスポンスを暗号化するモジュールである。このモジュールで行う暗号化は、Ｇｕｉｌｌｏｕ－Ｑｕｉｓｑｕａｔｅｒ認証で使用する法数のもとでの、鍵生成部１０５で生成される鍵とレスポンス生成部１２３が生成したレスポンスとの剰余演算である。

［鍵生成部１０５］：暗号部１０４で使用される暗号鍵を生成するモジュールである。このモジュールはＳＨＡ－１等のハッシュ関数で構成されている。後述する前鍵記憶部１０８に記憶されている前鍵と、鍵生成用データ記憶部１０９に記憶されているデータに、このハッシュ関数を適用した結果が鍵となる。

［前鍵生成部１０６］：鍵生成部１０５での鍵の生成に使用される前鍵を生成するモジュールである。生成する前鍵を攻撃者に予測されないよう、乱数生成器等を使って前鍵を生成する。

【００７９】

前鍵は、データ検証器２００に送られ、データ生成器１００とデータ検証器２００の間で共有される。共有されている間は、データ検証器２００に前鍵を送る必要はない。いつ共有をやめて、新しい前鍵をデータ検証器２００に送るかは前鍵生成部１０６が決定する。そのため前鍵生成部１０６は、時計を内蔵しており、以前前鍵を送付してから一定時間が過ぎると、新たな前鍵を生成する。

［前鍵暗号部１０７］：前鍵を暗号化し、その結果を送信部１０２に送るモジュールである。このモジュールでの暗号化はＲＳＡ暗号を用いる。このモジュールはＲＳＡ暗号を実施するプログラムと、暗号鍵を内蔵している。

［前鍵記憶部１０８］：前鍵生成部１０６が作成した前鍵を記憶するモジュールである。このモジュールが記憶している前鍵は、鍵生成部１０５が鍵を生成する際、および、前鍵暗号部１０７が前鍵を暗号化する際に参照される。

［鍵生成用データ記憶部１０９］：鍵生成部１０５での鍵の生成に使用されるデータを記憶しているモジュールである。具体的には、認証実行日時の情報と、このデータ生成器１００の識別子を記憶している。前者のデータは、データ検証器２００から送信されるものである。後者のデータは、本データ生成器１００に埋め込まれたものであり、送信部１０２を通して、データ検証器２００に送信される。

【００８０】

データ検証器２００が含むモジュールの役割について以下に記す。

［送信部２０１］：データを通信に適したフォーマットに変換しデータ生成器１００に送付する。

［受信部２０２］：データ生成器１００から送付されたデータを受け取り、通信用フォーマットからデータ検証器２００内部のフォーマットに変換した後、受信したデータをデータ検証器２００内のほかのモジュールに振り分ける。

［コミットメント記憶部２２０］：このモジュールにデータ生成器１００から送られたコミットメントを記憶する。ここに記憶されているデータは、レスポンス検証部２２１がレスポンスを検証する際に参照される。

［チャレンジ記憶部２２２］：このモジュールにデータ生成器１００にレスポンスを要求するチャレンジが記憶されている。ここに記憶されているデータは、送信部２０１を通してデータ生成器１００に送られる。また、レスポンス検証部２２１がレスポンスを検証する際に参照される。

［復号部２０４］：データ生成器１００から送信されたデータに含まれる暗号化されたレスポンスを復号するモジュールである。ここで行われる復号は、レスポンス検証部２２１でのレスポンスの検証に使われる法数のもとで、暗号化された

レスポンスを鍵生成部２０６で生成される鍵で割る演算である。

［レスポンス検証部２２１］：復号部２０４で復号したレスポンスの正当性を検証するモジュールである。このモジュールでは、コミットメント記憶部２２０に記憶されているコミットメント、チャレンジ記憶部２２２に記憶されているチャレンジに対して、復号部２０４で復号されたレスポンスが正当なものであるかどうかを検査する。

［鍵生成部２０６］：復号部２０４が使用する復号鍵を作成するモジュールである。データ生成器１００の鍵生成部１０５が持つのと同じハッシュ関数で構成されている。後述する前鍵記憶部２０７に記憶されている前鍵と、鍵生成用データ記憶部２０９に記憶されているデータに、このハッシュ関数を適用した結果が鍵となる。

［前鍵記憶部２０７］：前鍵復号部２０８が復号した前鍵を記憶するモジュールである。このモジュールが記憶している前鍵は、鍵生成部２０６が鍵を生成する際に参照される。

［前鍵復号部２０８］：前鍵は暗号化された状態でデータ生成器１００から送信される。このモジュールは、暗号化された前鍵を復号する。このモジュールでの復号にはＲＳＡ復号を用いる。その復号鍵は、データ生成器１００の前鍵暗号部１０７が保持する暗号鍵に対応する復号鍵であり、本モジュールはこの復号鍵を内蔵している。

［鍵生成用データ記憶部２０９］：鍵生成部２０６での鍵の生成に使用されるデータを記憶しているモジュールである。具体的には、認証実行日時の情報と、署名を生成したデータ生成器１００の識別子を記憶している。前者のデータは、本データ検証器２００に付随したクロックから取り出される。後者のデータは、データ生成器１００から証明データとともに送信される。

【００８１】

本実施例の動作について説明する。

【００８２】

本実施例は、大まかには、データ生成器１００がコミットメントをデータ検証器２００に送信し、データ検証器２００がデータ生成器１００にチャレンジを含

むデータ（チャレンジデータと呼ぶ）を送付し、データ生成器１００がデータ検証器２００にレスポンスを含むデータ（レスポンスデータと呼ぶ）を返信し、データ検証器２００でレスポンスデータの正当性を検査するというステップを踏む。

【００８３】

データ生成器１００がコミットメントを作成するときの動作を以下に示す。このコミットメント作成動作は簡潔なのでとくに図示することはしない。

［ステップ１］：乱数生成部１２０でコミットメント用の乱数を生成し、乱数記憶部１２１に記憶する。

［ステップ２］：乱数記憶部１２１に記憶されている乱数からコミットメント生成部１２２でコミットメントを作成する。

［ステップ３］：生成したコミットメントを送信部１０２からデータ検証器２００に送付する。

【００８４】

コミットメントを受け取ったデータ検証器２００の動作を以下に示す。このときのデータ検証器２００の動作も簡潔なのでとくに図示することはしない。

［ステップ１］：受信部２０１で受信したコミットメントをコミットメント記憶部２２０に記憶する。

［ステップ２］：チャンレンジを生成し、チャレンジ記憶部２２２にチャレンジを記憶する。

［ステップ３］：データ検証器２００が内蔵している時計から現在時刻情報を取り出し、それを認証実行時刻として鍵生成用データ記憶部２０９に記憶する。

［ステップ４］：チャレンジ記憶部２２２に記憶されているチャレンジと、鍵生成用データ記憶部２０９に記憶されている認証実行時刻とからチャレンジデータを作成し、送信部２０１からデータ生成器１００に送付する。

【００８５】

チャレンジデータを受け取ったデータ生成器１００の動作を以下に示すに示す。また、この動作の手順を記述したフローチャートを図８に示す。

［ステップＳ１４１］：受信部１０１で受信したチャレンジデータから、認証実

行時刻を取り出し、鍵生成用データ記憶部１０９に記憶する。

［ステップＳ１４２］：受信部１０１で受信したチャレンジデータから、チャレンジを取り出してレスポンス生成部１２３に送付し、レスポンス生成部１２３で、チャレンジと乱数記憶部１２１に記憶されている乱数とからレスポンスを作成する。

［ステップＳ１４３］：もし、新しい前鍵の生成が必要なら、前鍵生成部で前鍵１０６を作成し、前鍵記憶部１０８に記憶する。必要でなければ、ステップＳ１４５へ進む。

［ステップＳ１４４］：前鍵暗号部１０７で前鍵記憶部１０８に記憶されている前鍵を暗号化する。

［ステップＳ１４５］：鍵生成部１０５で、前鍵記憶部１０８に記憶されている前鍵と、鍵生成用データ記憶部１０９に記憶されている認証実行日時と本データ生成器１００の識別子から、鍵を生成する。

［ステップＳ１４６］：レスポンス生成部１２３で生成されたレスポンスを、鍵生成部１０５で生成された鍵を用いて、暗号部１０４で暗号化する。

［ステップＳ７］：暗号部１０４で暗号化されたレスポンスと、もしあれば前鍵暗号部１０７で暗号化された前鍵と、鍵生成用データ記憶部１０９に記憶されている本データ生成器１００の識別子とからレスポンスデータを作成し、送信部１０２からデータ検証器２００に送付する。

【００８６】

レスポンスデータを受け取ったデータ検証器２００の動作を以下に示す。また、この動作の手順を記述したフローチャートを図９に示す。

［ステップＳ１５１］：受信部２０２で受信したレスポンスデータから、レスポンスを生成したデータ生成器１００の識別子を取り出し、鍵生成用データ記憶部２０９に記憶する。

［ステップＳ１５２］：レスポンスデータに暗号化された前鍵が含まれていれば、それを取り出し、前鍵復号部２０８で復号し、その結果を前鍵記憶部２０７に記憶する。もし、暗号化された前鍵が含まれていなければ、何もせずステップＳ１５３へ進む。

［ステップＳ１５３］：鍵生成部２０６で、前鍵記憶部２０７に記憶されている前鍵と、鍵生成用データ記憶部２０９に記憶されている認証実行日時とデータ生成器１００の識別子から、鍵を生成する。

［ステップＳ１５４］：レスポンスデータから暗号化されたレスポンスを取り出し、鍵生成部２０６で生成された鍵を使用して、復号部２０４で復号する。

［ステップＳ１５５］：復号部２０４での復号の結果が、チャレンジ記憶部２２２に記憶されているチャレンジおよびコミットメント記憶部２２０に記憶されているコミットメントに照らして正しいものあるかどうかを検査する。

【００８７】

データ検証器２００が、ステップＳ１５５の検査で、正しいレスポンスあることが確認できた場合、データ検証器２００にとっては、以下のことが保証される。

【００８８】

１．データ生成器１００が作成したレスポンスが、チャレンジおよびコミットメントに対して正しい署名であること。

２．データ検証器２００が送付した認証実行日時が、差し替えられることなくデータ生成器１００に届いたこと。

３．受け取ったデータ生成器１００の識別子が、レスポンスを生成したデータ生成器１００と同一のものであること。

【００８９】

【発明の効果】

以上説明したようにこの発明によれば主検査対象データの検証手続に関連して副検査対象の真正性を検査することができ、その際、ハッシュ値等の冗長データを付加する必要がない。

【図面の簡単な説明】

【図１】　本発明の第１の実施例の構成を全体として示すブロック図である。

【図２】　上述第１の実施例のデータ生成処理を説明するフローチャートである。

【図３】　上述第１の実施例のデータ検証処理を説明するフローチャートである。

【図４】　本発明の第２の実施例の構成を全体として示すブロック図である。

【図５】　上述第２の実施例のデータ復号処理を説明するフローチャートである。

【図６】　上述第２の実施例のデータ検証処理を説明するフローチャートである。

【図７】　本発明の第３の実施例の構成を全体として示すブロック図である。

【図８】　上述第３の実施例のレスポンス生成処理を説明するフローチャートである。

【図９】　上述第３の実施例のレスポンス検証処理を説明するフローチャートである。

【図１０】　上述第２の実施例の変形例を説明する図である。

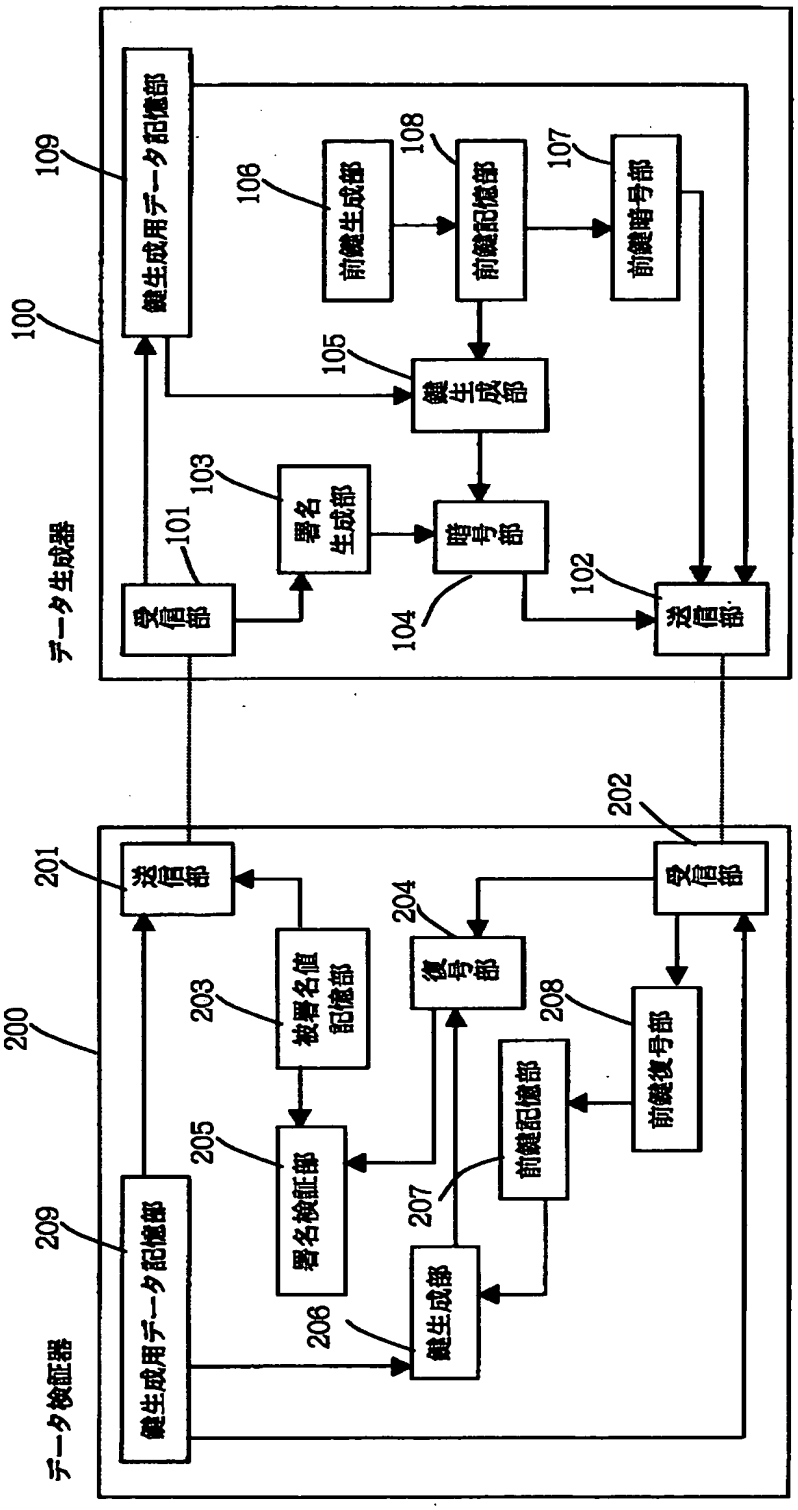
【符号の説明】

１００　データ生成装置
１０１　受信部
１０２　送信部
１０３　署名生成部
１０４　暗号部
１０５　鍵生成部
１０６　前鍵生成部
１０７　前鍵暗号部
１０８　前鍵記憶部
１０９　鍵生成用データ記憶部
１１０　暗号文復号部
１２０　乱数生成部
１２１　乱数記憶部

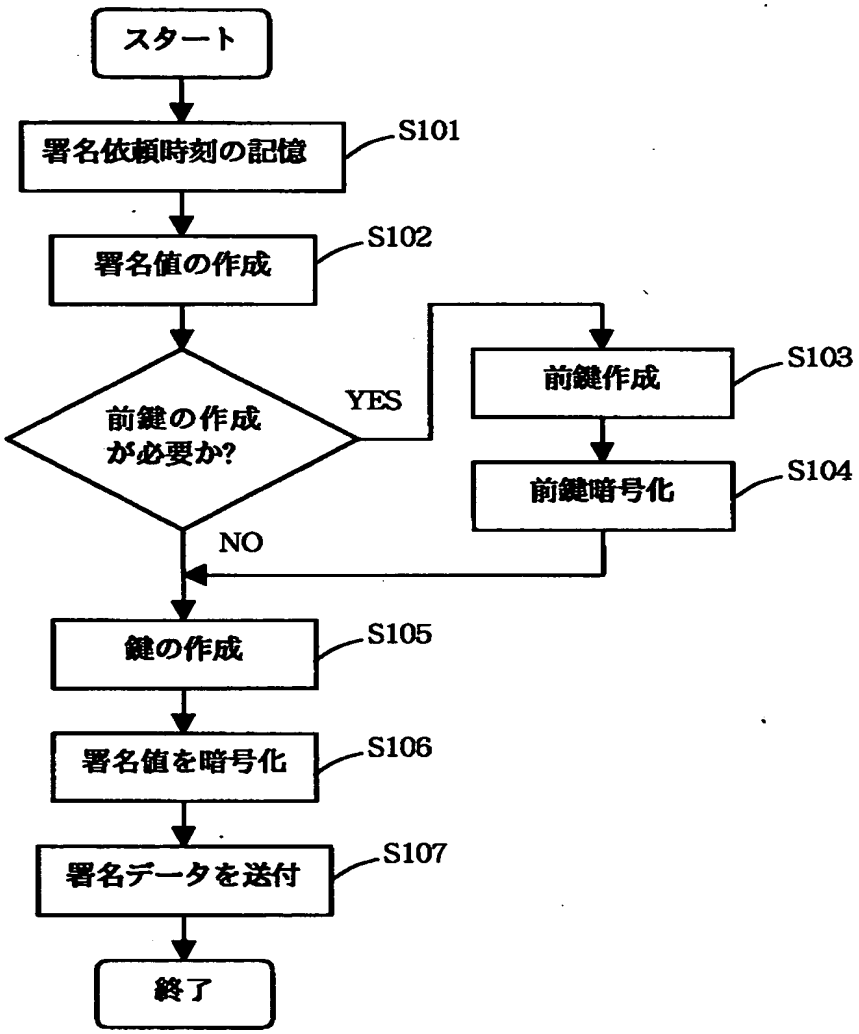
１２２　コミットメント生成部
１２３　レスポンス生成部
２００　データ検証器
２０１　送信部
２０２　受信部
２０３　被署名値記憶部
２０４　復号部
２０５　署名検証部
２０６　鍵生成部
２０７　前鍵記憶部
２０８　前鍵復号部
２０９　鍵生成用データ記憶部
２１０　暗号文記憶部
２１１　復号結果検証部
２２０　コミットメント記憶部
２２１　レスポンス検証部
２２２　チャレンジ記憶部

【書類名】　　図面

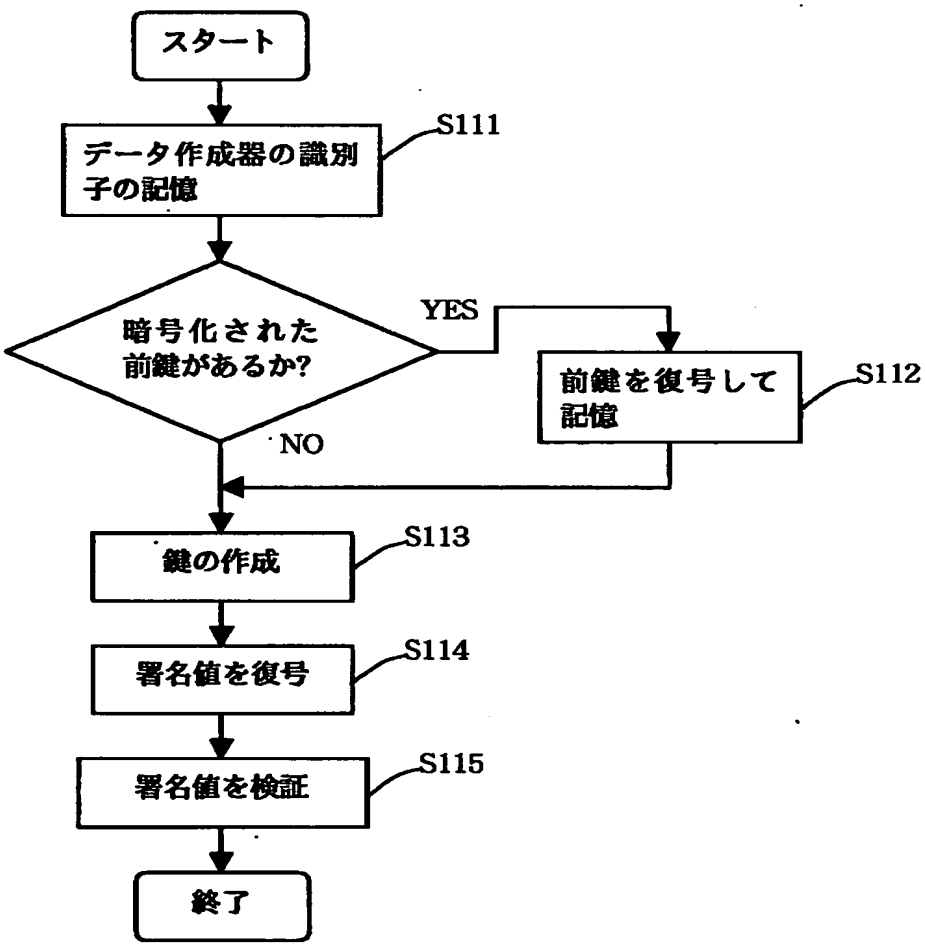
【図１】


データ生成器
データ検証器
鍵生成用データ記憶部
前鍵生成部
前鍵記憶部
前鍵暗号部
鍵生成部
署名生成部
暗号部
受信部
送信部
鍵生成用データ記憶部
被署名値記憶部
署名検証部
鍵生成部
復号部
前鍵記憶部
前鍵復号部
受信部
送信部
100
101
102
103
104
105
106
107
108
109
200
201
202
203
204
205
206
207
208
209

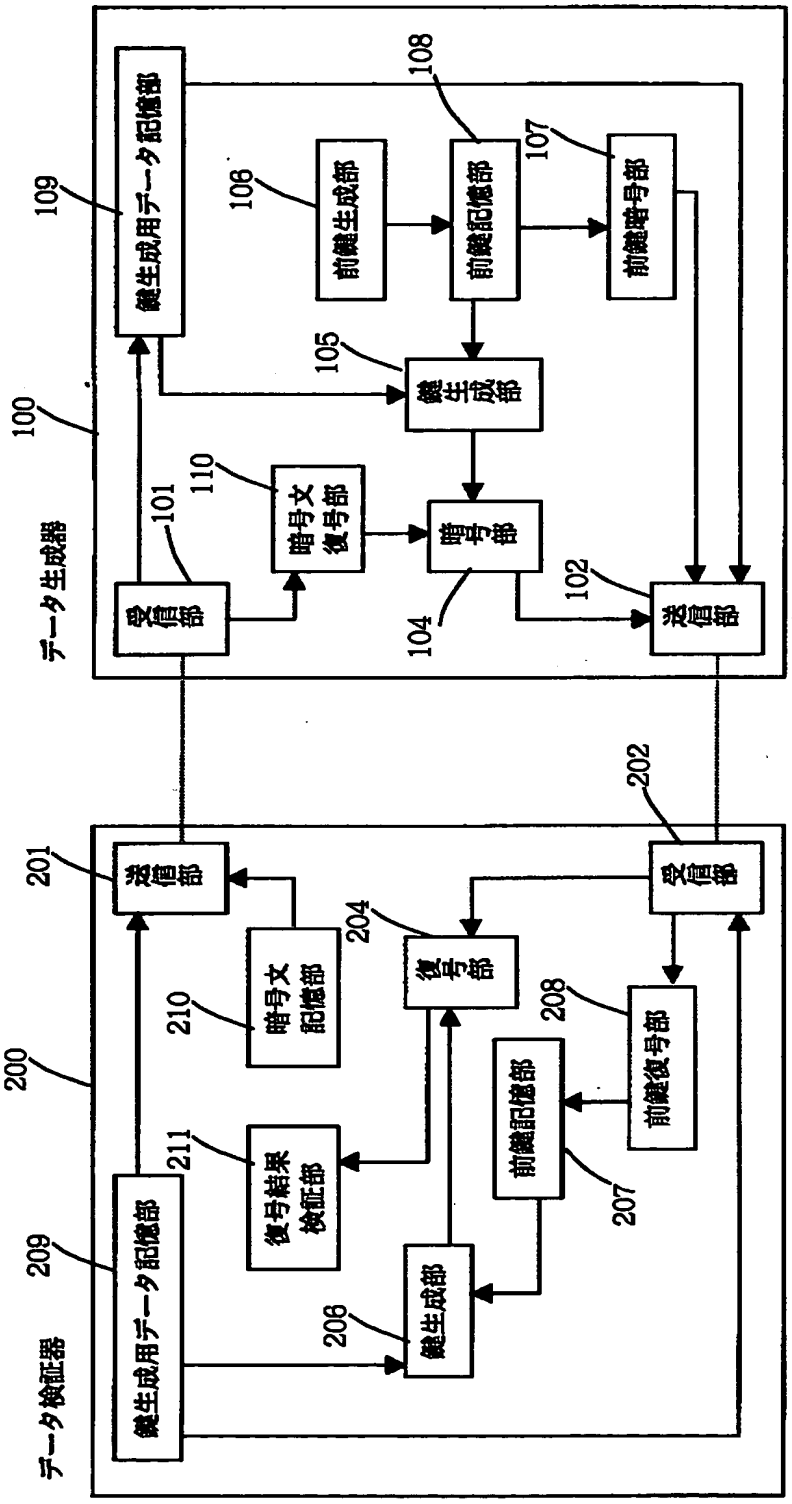
【図２】


スタート
署名依頼時刻の記憶
S101
署名値の作成
S102
前鍵の作成
が必要か?
YES
前鍵作成
S103
前鍵暗号化
S104
NO
鍵の作成
S105
署名値を暗号化
S106
署名データを送付
S107
終了

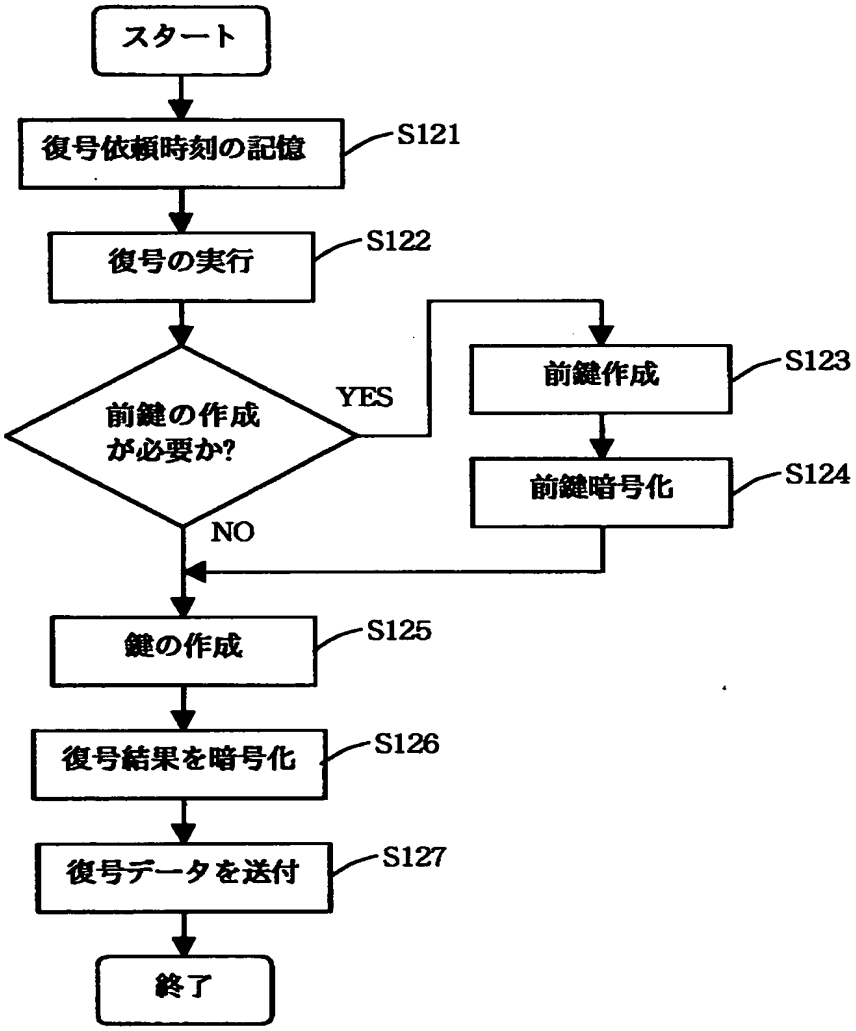
【図３】


スタート
データ作成器の識別子の記憶
S111
暗号化された前鍵があるか?
YES
NO
前鍵を復号して記憶
S112
鍵の作成
S113
署名値を復号
S114
署名値を検証
S115
終了

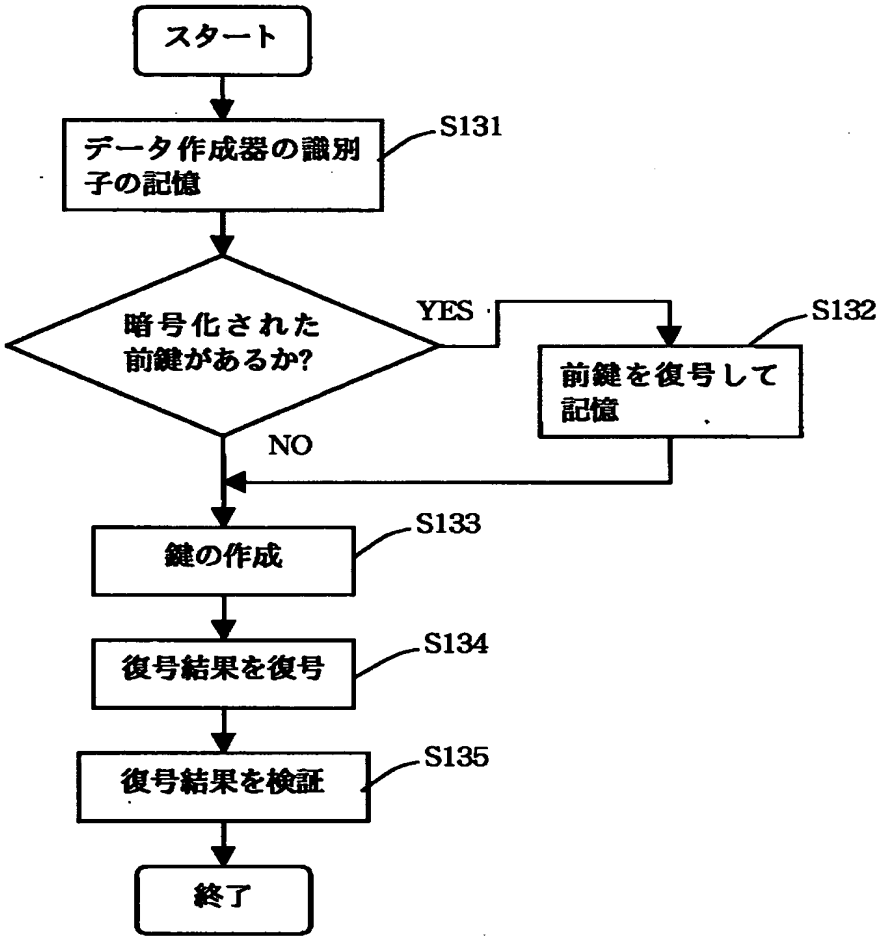
【図４】


データ生成器
100
鍵生成用データ記憶部
109
前鍵生成部
106
前鍵記憶部
108
前鍵暗号部
107
鍵生成部
105
暗号文復号部
110
暗号部
104
受信部
101
送信部
102
データ検証器
200
送信部
201
受信部
202
暗号文記憶部
210
復号部
204
前鍵復号部
208
前鍵記憶部
207
復号結果検証部
211
鍵生成部
206
鍵生成用データ記憶部
209

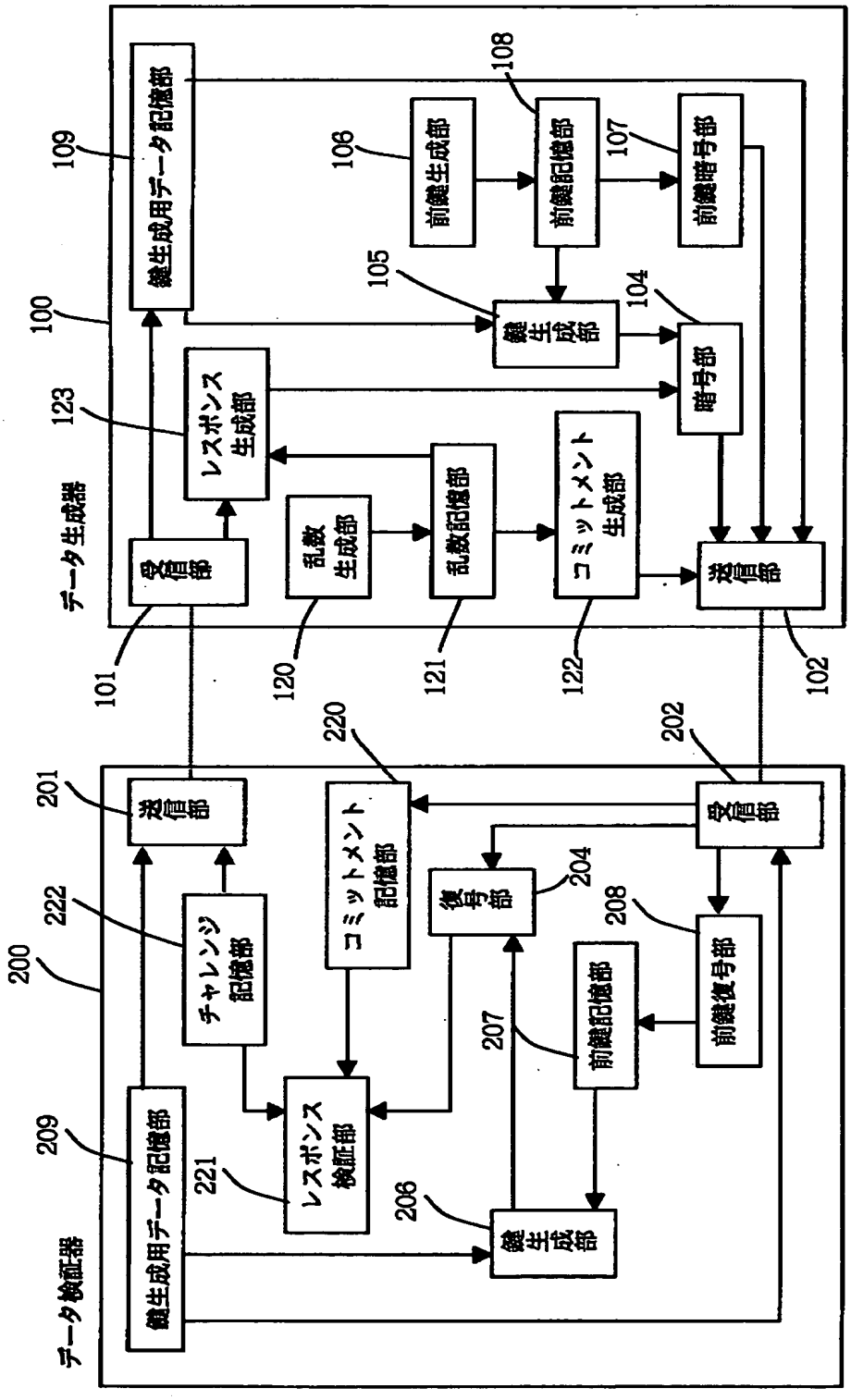
【図５】


スタート
復号依頼時刻の記憶
S121
復号の実行
S122
前鍵の作成が必要か?
YES
NO
前鍵作成
S123
前鍵暗号化
S124
鍵の作成
S125
復号結果を暗号化
S126
復号データを送付
S127
終了

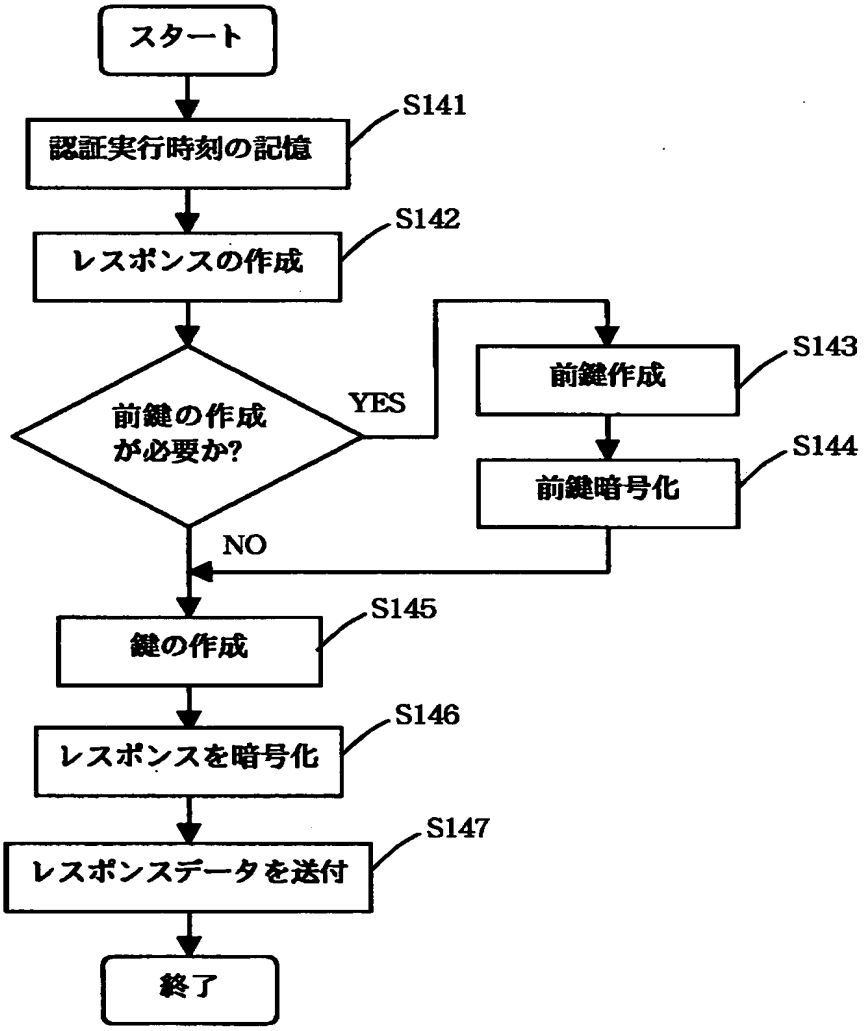
【図６】


スタート
データ作成器の識別子の記憶
S131
暗号化された前鍵があるか?
YES
S132
前鍵を復号して記憶
NO
鍵の作成
S133
復号結果を復号
S134
復号結果を検証
S135
終了

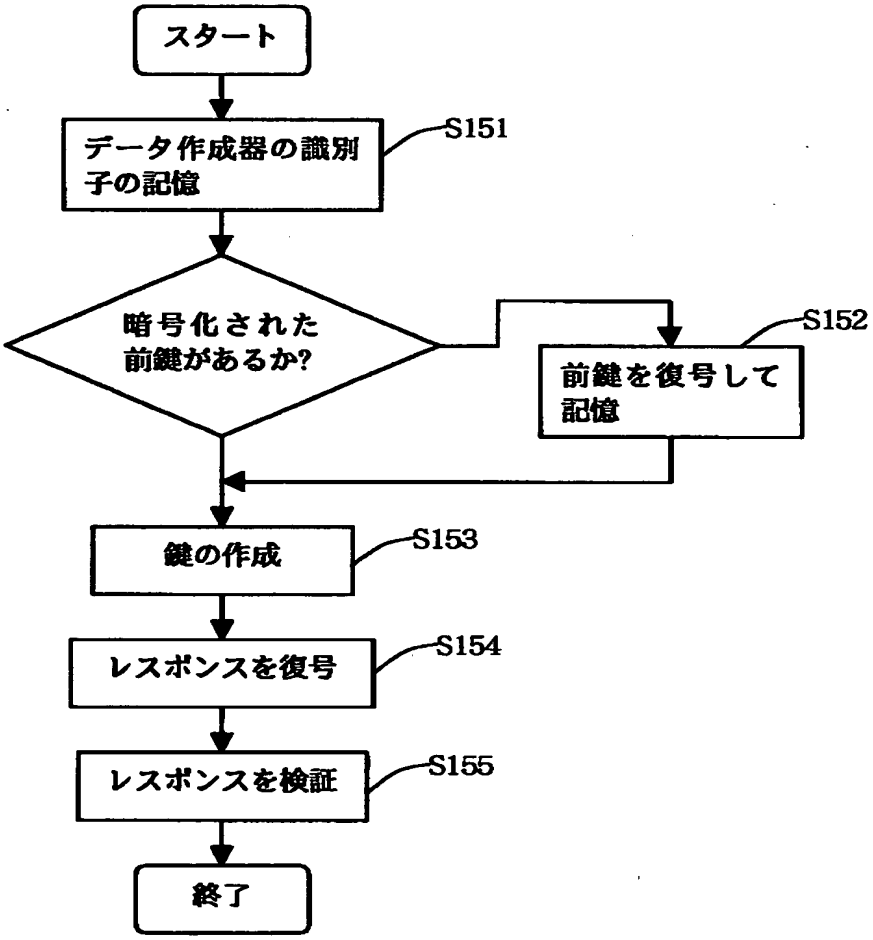
【図７】


データ生成器
データ検証器
鍵生成用データ記憶部
前鍵生成部
前鍵記憶部
前鍵暗号部
鍵生成部
暗号部
レスポンス生成部
乱数生成部
乱数記憶部
コミットメント生成部
受信部
送信部
100
101
102
104
105
106
107
108
109
120
121
122
123
200
201
202
204
206
207
208
209
220
221
222
コミットメント記憶部
復号部
チャレンジ記憶部
レスポンス検証部
前鍵復号部

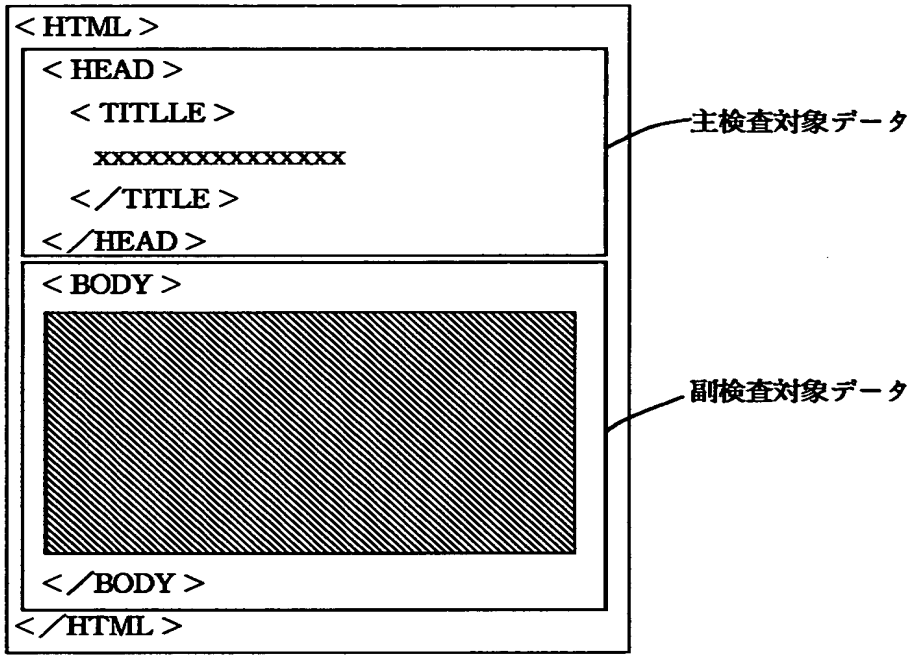
【図８】


スタート
S141
認証実行時刻の記憶
S142
レスポンスの作成
前鍵の作成
が必要か?
YES
S143
前鍵作成
S144
前鍵暗号化
NO
S145
鍵の作成
S146
レスポンスを暗号化
S147
レスポンスデータを送付
終了

【図９】


スタート
データ作成器の識別子の記憶
S151
暗号化された前鍵があるか?
S152
前鍵を復号して記憶
鍵の作成
S153
レスポンスを復号
S154
レスポンスを検証
S155
終了

【図１０】


<HTML>
<HEAD>
<TITLLE>
xxxxxxxxxxxxxxx
</TITLE>
</HEAD>
<BODY>
</BODY>
</HTML>
主検査対象データ
副検査対象データ

【書類名】　要約書

【要約】

【課題】　データの完全性の保証を簡易に行う。

【解決手段】　データ検証器２００が被署名値と署名依頼時刻とから署名作成依頼を作成し、データ生成器１００に送付する。データ生成器１００が、署名作成依頼から、被署名値を取り出し、その署名生成部１０３が、被署名値に対する署名値を作成する。鍵生成部１０５が、前鍵と、署名作成依頼中の署名依頼時刻と、データ生成器１００の識別子から、鍵を生成し、暗号部１０４が署名値を暗号化する。この後、暗号化署名値等をデータ検証器２００に返信する。データ検証器２００は、鍵生成部２０６で、前鍵と、署名依頼時刻と、データ生成器１００の識別子とから、復号鍵を生成し、さらに、暗号化署名値を取り出し、復号部２０４で復号する。署名検証部２０５が復号の結果が正しい署名であるかどうかを検査する。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５４９６〕

１．変更年月日　　１９９６年　５月２９日
［変更理由］　住所変更
住　所　東京都港区赤坂二丁目１７番２２号
氏　名　富士ゼロックス株式会社